Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 3110-3116

Research Article

Controlling Internet of Things with different platforms: Security and Privacy challenges

Nora N. ALshehri[1], Mohammed A. AlZain[1], Mehedi Masud[1,*], NZ Jhanjhi[2], Jehad Al-Amri[1], Mohammed Baz[1]

[1]College of Computers and Information Technology, Taif University,
P.O. Box 11099, Al-Hawiya-Taif, 21944, Saudi Arabia
[2]School of Computer Science and Engineering, SCE, Taylor's University, 47500, Malaysia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract

The Internet of Things (IOT) is one of the most important topics these days. It contains huge numbers of devices connected to each other with a very accurate access control through advanced and trusted control. IOT aims to use easy and achieve high security for the users. Based on that, this paper surveys recent research related to controlling three generations of network types have passed through the IOT which services the client in accessing or controlling their resources. In addition, this work aims to describe centralized framework (such as cloud computing), decentralized system (like edge computing), distributed network (Blockchain technology), and smart contract in IOT with the description of their security and privacy challenges.

Keywords: Centralized system, Decentralized system, Internet of things, Blockchain.

1. Introduction

Recently, there is a huge development of system administration's innovations (e.g., Wi-Fi, Zigbee, Bluetooth) , a developing number of items (e.g., sensors, actuators, smart gadgets) are being associated with the Internet these days, prompting the idea of the Internet of things (IoT) [1, 2]. As of late, the fast improvement of the IOT has advanced social and financial improvement [3, 4]. The report reasons that in excess of 100 billion gadgets, including cell phones and wearable gadgets, clinical gadgets, electrical apparatuses, modern sensors, observation cameras, vehicles, and dress, will be associated with the Internet of 16 by 2045. These offices completely mechanize the review, the executives, and upkeep of the first workforce[5, 6].

Presently a day, an individual is being encircled by many billions of IoT gadgets to improve natural life and simpler [7] yet for the equivalent, the individual is being followed and infringing space of private of the individual that prompts more issues in security and wellbeing areas[8],[9]. Because of the open climate of the framework where the gadgets are associated and interconnected with the Internet, unapproved modification, admittance to confidential information, or even forswearing of administration might be a lot simpler [10],[11]. Therefore, the basic troubles in using IoT will be: Privacy, Security. To crush these issues, an Access Control Systems are to be portrayed [12].

One of the hot exploration themes now a days is IOT. Numerous specialists over the globe are utilizing their endeavours to report different security challenges of security in IoT. Anyway, security of internet of things is an incredible test as a result of its heterogeneous nature[13]. Web of things being the mix of countless innovations, their own personal customary security and protection defects for all these advancements, which are to be tended to in IoT setting [14]. Smart contract is program code that stored on blockchain, utilized to perform any task. The purpose from smart contract is organized between network part spit but in digital contract. Smart contract do not need third party.
This paper focuses on the controlling in internet of things without control centre. In addition, it aims to describe centralized framework, decentralized system, distributed network, and smart contract in IOT with the description of their security and privacy challenges.

The remainder of this paper is organized as follows. Section 2 describes the beginning of Access control in IOT. Section 3 discusses centralized system with the architecture and style of IOT. Section 4 shows decentralized system and edge computing in IOT. Section 5 presents Blockchain technology. Section 6 will conclude the paper.

2. Background (Access control: Preliminary)

Access control is an instrument that restricts the tasks or exercises of a genuine client[15].The entrance functionalities of control increment with consolidation of appointment module, where the designation is a cycle for allocating impermanent authorizations to a client [16]. For instance, a delegator can carry on as an individual

who moves his authorizations to someone else. The individual, who gets these authorizations, is known as the delegate. A client delegates consents in the reaction of either a question or a function. In function-based consent appointment, authorizations are assigned to a particular client in the reaction of an event2. In inquiry based authorization appointment, the client demands for consent on an asset from the proprietor[17]. Exemplary access-control records (ACLs) determine an activity, a subject, an article, and the "affirm or deny" choice. for the internet of things they are not expressive enough [18].

Shockingly little consideration has been paid to get to control-strategy detail (communicating which specific clients, in which settings, are allowed to get to an asset) or validation (confirming that clients are who they guarantee to be) in the IoT[19]. This situation is upsetting in light of the fact that the qualities that make the IoT unmistakable from earlier registering areas require a re-examining of access control and verification[19]. Conventional gadgets like PCs, telephones, tablets, and keen watches are commonly utilized by just a solitary individual. Hence, when a client confirms to their own personal gadget, negligible extra access control is mandatory[19]. These gadgets have consoles and screens, so the cycle of validation regularly includes passwords, PINs, unique mark biometrics, or comparative methodologies[3].

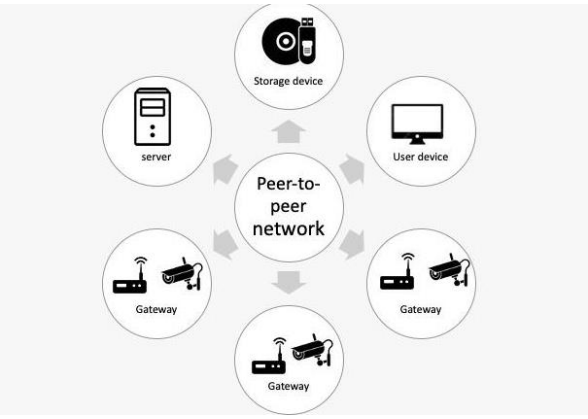

Figure 1 Illustration of IOT system[20].

3. Internet of Things IOT.

This section will discuss what is the IOT? , with a brief details of its elements and architecture.

3.1 System architecture of IOT .

As outlined in Fig. 1, the IOT framework considered in this paper comprises of countless workers, stockpiling gadgets, IOT passages and client gadgets, which are associated together through a shared (P2P) organization. Additionally, present in the framework are various IOT gadgets (e.g., sensors and actuators), which are associated with the P2P network through the IOT passages. The principle parts of the companions are clarified as follows:
1. Server: A worker is a gadget or a bunch of gadgets that can communicate with the IOT gadgets and capacity gadgets to give an assortment of administrations (e.g., keen home) for clients. Cooperation between the workers and different companions (e.g., IOT gadgets, stockpiling gadgets) incorporate gathering natural information from the sensors, sending orders to the actuators to play out some activity, questioning information from or putting away information to the capacity gadgets, and so forth[20].

2.Storage gadget: A capacity gadget can store information for different companions of the framework, similar to the workers, sensors and clients. Different information can be put away on the capacity gadgets, similar to the application information of the workers, natural information assembled by the sensors, client profiles, User gadget: A client gadget is a gadget (e.g., PCs, PCs, advanced cells) through which clients can appreciate the administrations (e.g., checking the current temperature of his/her own personal house) gave by the workers and read information from or compose information to the capacity gadgets[20].

3. IOT entryway: Each IOT door associates a group of IoT gadgets to the P2P network through short-range correspondence advancements like Bluetooth, Wi-Fi and Zigbee, and fills in as the administration operator for these IoT gadgets simultaneously.

4. IOT tool: The IoT gadgets in the framework principally incorporate sensors, which can see ecological information (e.g., temperature) and send this information to the workers or capacity gadgets for additional

utilization, and actuators, which can play out certain activities (e.g., turning broadcasting live conditioner) once getting an order from clients. and so forth[20].

4.Centralized system

Incorporated admittance control frameworks give security of information s by giving or disavowing the rights to get to the information through the clients with a drawback of single purpose of disappointment [7], while the decentralized admittance control frameworks supplant the hindrance of brought together frameworks with different spots giving the entrance authorizations to the clients. Today, the use of decentralized frameworks is expanding quickly as a result of its preferences over brought together frameworks [8], [9]. The centralized stuff such as IOT can be unmistakably perceived and where its execution is truly required. The entrance control strategy ought to be so that the clients will be able to control their own personal protection. another entrance control technique should be built up that gives exact outcomes for the decentralized organizations[20].

Solution of centralized not just builds the organization unpredictability by inconclusive quantities of additional associations with the cooperation the executives' stages, yet in addition requires extra assets and endeavours on each synergistic IoT gadget, including power utilization, memory space, programming multifaceted nature, and so forth, which are incredibly restricted on numerous battery-controlled gadgets. In addition, information islands shaped on brought together stages will in general build up their own personal environments as opposed to adjusting with others. In addition, unified arrangements have clear downsides when clients choose to supplant brilliant gadgets from various merchants. Accordingly, the whole keen industry will be scattered and float away from a definitive objective of carrying comfort to individuals' life. Consequently, decentralized coordinated effort components inspired by these previous realities are getting increasingly more attentions[21].

There is likewise the issue that the current approval structure can't adequately give an effectively adaptable and sensible access control system to furnish dynamic versatility with numerous wise terminals and intelligent administrations, which additionally can't uphold access control necessities of circulated IoT conditions .Due to the wide conveyance and complex climate, it was restricted in processing and capacity assets, for example, cloud computing[4],[22] .

It additionally has focal points, edge computing addresses the issues of industry digitization in rapid association, constant assistance, information enhancement, application insight, and it likewise faces numerous security challenges [23]. Commonplace personality the executives and access control systems depend on a brought together confided in substance. As the registering intensity of the terminal builds, there are more occasions to carry insight to the terminal itself, particularly as far as security and access control rationale[4].

An example on centralized system with internet of things:
Model computing of cloud on IOT is the intelligent health, In the intelligent health shrewd, a huge number of IoT devices assemble Smart Health Records[24] and impart them to a cloud specialist co-op (CSP) for limit and sharing The healthy circle of data sharing structure.

a Secure Smart Health system [25]with insurance careful complete check and access control in web of things
The joining of IoT and commuting of cloud progressions has become a promising plan. As showed up in Fig. 2, particular sorts of wise devices can accumulate SHRs and reallocate them to the cloud labourer for limit and sharing[20].

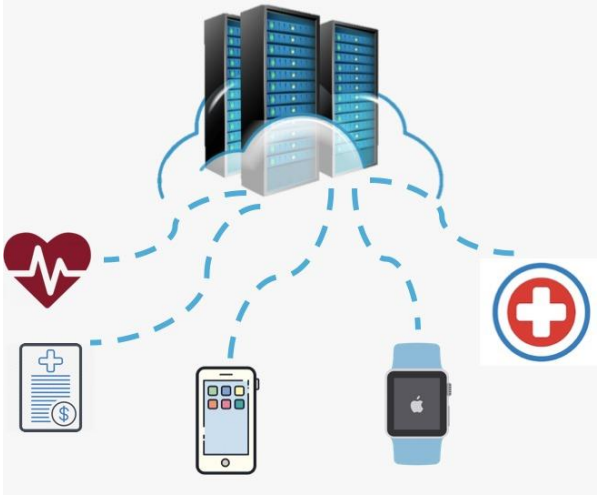

Figure 2. cloud computing and smart health [20].

4. Decentralized system in IOT

Computing of edge is the new worldview for a heap of strategic applications. Computing of edge has cut a specialty in the innovative world because of its colossal performing abilities of giving constant information investigation, low operational cost, high adaptability, diminished inactivity and improved nature of administration[26].

Computing of edge follows a decentralized design with information handling at the edge of the network hubs to settle on self-sufficient choices Accordingly, the applications running on computing of edge will perform activities locally prior to associating with the cloud, subsequently decreasing organization overhead issues also as the security and protection issues. With the reconciliation of edge computing, the handling capacities are pushed to the edge of network gadgets, for example, advanced mobile phones, nodes of sensor ,and wearables, where information investigation and analytics of data furthermore, information age are performed which eliminates the need for a centralized framework[26].

A lot of IoT applications, for example, smart town, the shrewd network, intelligent traffic signals, and savvy vehicles, are quickly redesigning their applications with edge computing , altogether improving reaction time just for conserving resources of network.

Independent of the way that EC moves the remaining task at hand from a unified cloud to the edge.as in the figure 3[27].

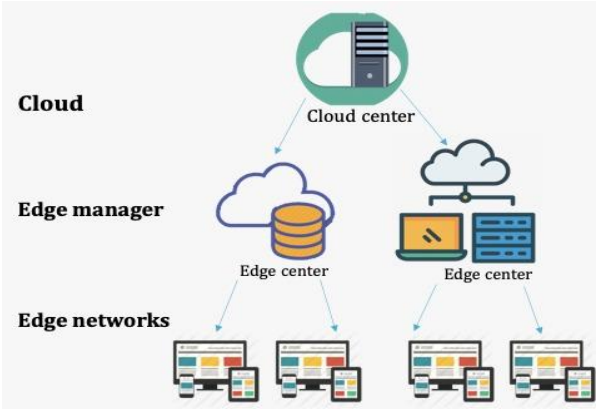

Figure 3.Adge computing Architecture[27].

5. Distributed Network

This part aims to add new modern technology with decentralized control systems.

Blockchain: Preliminary

Blockchain mechanism effectively accomplishes agreement among disseminated members with malignant hubs without the mediation of any trust middle person. Blockchain innovation has as of late been applied in the web of things to give safety and defines assurance, due to its comparative geography to the Internet of things[28]. Blockchain is a shared organization that comprises of various hubs and takes a shot on protocol of cryptographic algorithms [12],[29],[30]. By confirming the exchanges and passing between these nodes subsequently, these nodes handle the communication. The highlights of the blockchain makes it intriguing and simple to utilize. Blockchain is an annex just information base innovation[12]. Thus, once the information is embedded into the data set, it can't be altered or erased. Anybody can see all the exchanges, which is only the people who are in blockchain technology which is of the general type which is mainly Blockchain technology. [31], [12].
A Blockchain is a public archive of information. It is a safe, effectively accessible, decentralized information base. Clients acknowledge the data and investigate the data if it is secure where It depends on principle of trustless , with no outsider connection or any other party [12]. Toward the start, it is principally evolved to give secure digital currencies such as Bitcoins, where these days the examines are attempting to enforce blockchain to different domain[12].
the blockchain is separated to two types of blockchain: public and private [32]. Each client is allowed to send exchanges to view information. It is the blockchain technology, which is of the public type. As for the private type, it is only allowed for those who are predefined within the chain to conduct exchanges [12].
it is the most generally spread technology this days for its potential benefits [12].

The Internet of Things (IoT) is venturing out of its early stages into full development and building up itself as a feature of things to come Internet. One of the specialized difficulties of having billions of gadgets conveyed overall is the capacity to oversee them. Despite the fact that entrance the board innovations exist in IoT, they depend on incorporated models which present another assortment of specialized constraints to oversee them internationally[33].

Before the creation of the blockchain, overseeing different exercises and activities over the Internet was accomplished through a unified worker to ensure the data do not non-repudiation. A gathering of appropriated substances couldn't confirm exchanges without utilizing the concentrated authority [34]. The Byzantine Generals Problem (BGP) issues [35],[36] are necessary trust must be created if there is no trust between the carrier parties and deals with the correspondence cycle. [37].

Smart contracts enable documented terminology for understanding that must be supported without an external trusted person and is an integral part of the blockchains.
smart contracts comprising of exchanges are basically replicated , stored, replicated and refreshed in distributed blockchains[38].

An example of using blockchain technology and its mixing with the IOT it achieved our three security goals, which are integrity, availability and confidentiality.
In this structure , it proved that the secure, trusted, verifiable and resistance of tamper of the decentralized environment have been achieved with blockchain technology[39].

Permission of delegation and control of access to the Internet of Things was done by blockchain technology. By delegating permissions to IoT devices and IoT users, they were granted other additional permissions through a number of permissions assigned to them, and this by using blockchain technology to implement the authorization of permissions. Access to the source is through a smart contract that the owner of the Internet of things device creates on the source of the blockchain.
Where an IoT user or IoT device sends the request on the blockchain to the source of the smart contract.
Before activating the permission, the blockchain must verify the Delegates platform[39].

The following stage of improvements is to combine the IoT with blockchain innovation. In spite of that style of centralized IoT gives different advantages, it raises serious difficulties with respect to costs, security and with scalability[40].

Also, without a third party, the security issues with respect to the single purpose of disappointment will be wiped out [41].

6. Conclusion

It is clear that although the use of IOT has rapidly increased, access control in IOT is still considered the main issue in control center. It is clear in this research that there are three types of networks, which are distributed,

centralized and decentralized with the Internet of things, with the special examples of each network and the development that took place from one stage to the next. New that does not need a central system, which is blockchain technology. The determination of this work is to survey the research of different frameworks in IOT.

7. References:

1. Yaqoob, I., et al., Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 2017. **24**(3): p. 10-16.
2. Palattella, M.R., et al., Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, 2016 **34**(3): p. 510-527.
3. Bonneau, J., et al. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. in 2012 IEEE Symposium on Security and Privacy. 2012,IEEE.
4. Chen, C.-H., M.-Y. Lin, and C.-C. Liu, Edge computing gateway of the industrial internet of things using multiple collaborative microcontrollers. IEEE Network, 2018. **32**(1): p. 24-32.
5. Steiner, W. and S. Poledna, Fog computing as enabler for the Industrial Internet of Things. e & i Elektrotechnik und Informationstechnik, 2016. **133**(7): p. 310-314.
6. Yin, C., et al., Location privacy protection based on differential privacy strategy for big data in industrial internet of things. IEEE Transactions on industrial informatics, 2017. **14**(8): p. 3628-3636.
7. Lin, N. and W. Shi. The research on Internet of things application architecture based on web. in 2014 IEEE workshop on advanced research and technology in industry applications (WARTIA). 2014: IEEE.
8. AlZain, M.A., et al. Cloud computing security: from single to multi-clouds. in 2012 45th Hawaii International Conference on System Sciences. 2012: IEEE.
9. AlZain, M.A., B. Soh, and E. Pardede. Mcdb: using multi-clouds to ensure security in cloud computing. in 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. 2011: IEEE.
10. Mendez, D.M., I. Papapanagiotou, and B. Yang, Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879, 2017.
11. Alzain, M.A. and E. Pardede. Using multi shares for ensuring privacy in database-as-a-service. in 2011 44th Hawaii International Conference on System Sciences. 2011: IEEE.
12. Dukkipati, C., Y. Zhang, and L.C. Cheng. Decentralized, blockchain based access control framework for the heterogeneous internet of things. in Proceedings of the Third ACM Workshop on Attribute-Based Access Control. 2018.
13. Alshambri, H., et al., Cybersecurity attacks on wireless sensor networks in smart cities: an exposition. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 2020. **8**(1).
14. Ali, I., S. Sabir, and Z. Ullah, Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309, 2019
15. Sandhu, R.S. and P. Samarati, Access control: principle and practice. IEEE communications magazine, 1994. **32**(9): p. 40-48.
16. Wang, Q., N. Li, and H. Chen. On the security of delegation in access control systems. in European Symposium on Research in Computer Security. 2008: Springer.
17. Ali, G., et al., Blockchain based permission delegation and access control in Internet of Things (BACI). Computers & Security. **86**: p. 318-334.
18. M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, "Emerging Smart Logistics and Transportation Using IoT and Blockchain," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 58-62, June 2020, doi: 10.1109/IOTM.0001.1900097.
19. Almusaylim, Z. A., & Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless networks, 25(6), 3193-3204.
20. Zhang, Y., et al., Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 2018. **6**(2): p. 1594-1605.
21. Tang, B., et al. Iot passport: A blockchain-based trust framework for collaborative internet-of-things. in Proceedings of the 24th ACM symposium on access control models and technologies. 2019.
22. Al-Amri, B.O., et al., A Comprehensive Study of Privacy Preserving Techniques in Cloud Computing Environment. Advances in Science, Technology and Engineering Systems Journal, 2020. **5**(2): p. 419-

424.

23. Novo, O., Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 2018**5**(2): p. 1184-1195.
24. Samra, H.E., et al., A Conceptual Model for Cloud-Based E-Training in Nursing Education, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 295-310.
25. Samra, H., et al., Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems. Health Information Management Journal, 2019. **49**(2-3): p. 117-126.
26. El-Sayed, H., et al., Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. IEEE Access, 2017. **6**: p. 1706-1717.
27. Ren, Y., et al., Identity management and access control based on blockchain under edge computing for the industrial Internet of Things. Applied Sciences, 2019**9**(10): p. 2058.
28. Humayed, A., et al., Cyber-physical systems securityâ€”A survey. IEEE Internet of Things Journal, 2017. **4**(6): p. 1802-1831.
29. Faragallah, O.S., et al., Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications. IEEE Access, 2020.
30. Faragallah, O.S., et al., Efficiently Encrypting Color Images with Few Details based on RC6 and Different Operation Modes for Cybersecurity Applications. IEEE Access, 2020. **8**(1).
31. Alabdali, N.A., et al., BITCOIN AND DOUBLE-SPENDING: HOW PAVING THE WAY FOR BETTERMENT LEADS TO EXPLOITATION. Indian Journal of Computer Science and Engineering, 2020. **11**(1).
32. Dinh, T.T.A., et al. Blockbench: A framework for analyzing private blockchains. in Proceedings of the 2017 ACM International Conference on Management of Data. 2017.
33. A. P. Singh et al., "A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2020.3037889.
34. Stanciu, A. Blockchain based distributed control system for edge computing. in 2017 21st International Conference on Control Systems and Computer Science (CSCS). 2017: IEEE.
35. AlZain, M.A., et al., Byzantine Fault-Tolerant Architecture in Cloud Data Management. International Journal of Knowledge Society Research (IJKSR), 2016. **7**(3): p. 86-98.
36. AlZain, M.A., et al., Managing Multi-Cloud Data Dependability Faults, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 207-221.
37. Lamport, L., R. Shostak, and M. Pease, The Byzantine generals problem, in Concurrency: the Works of Leslie Lamport. 2019. p. 203-226.
38. Zheng, Z., et al., An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 2020 **105**: p. 475-491.
39. Ali, G., et al., Blockchain based permission delegation and access control in Internet of Things (BACI). Computers & Security, 2019. **86**: p. 318-334.
40. Atlam, H.F. and G.B. Wills, Technical aspects of blockchain and IoT, in Advances in Computers. 2019, Elsevier. p. 1-39.
41. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cybersecurity threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45(4), 3171-3189.